ICS613: **ICS/OT Penetration Testing & Assessments™**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Plan and execute safe, effective, and valuable penetration tests and security assessments using both passive and active techniques to assess operational resilience in ICS environments
- Tailor ICS penetration tests and security assessments to serve the customer's organizational and operational security objectives
- Collaborate with customers to identify realistic ICS attack scenarios targeting Crown Jewel Assets (CJA)
- Communicate and coordinate with stakeholders to define expectations, goals, and outcomes for ICS security assessments
- Understand the benefits of a top-down/bottom-up approach to active testing and how aligning penetration test methodologies to the ICS Cyber Kill chain provides appropriate adversary context to engagement activities, findings, and recommendations
- Evaluate tools and techniques for effectiveness and safety before applying them to ICS devices and networks
- Identify relevant targets and select applicable adversary TTPs for developing effective attack scenarios in ICS penetration tests and security assessments, regardless of industry sector
- Write and deliver timely status updates and accurate, actionable reports that support customer goals and outcomes

Industrial Control Systems (ICS) and Operational Technology (OT) are increasingly targeted by adversaries, yet traditional penetration testing approaches often focus on the wrong outcomes and can cause unintended disruptions with severe consequences—including production outages, injury to personnel, loss of life, and environmental hazards. ICS613: ICS/OT Penetration Testing & Assessments introduces engineering, operations, and security professionals with the mindset, methodologies, and techniques to safely and appropriately conduct penetration tests and security assessments, identify practical mitigations, and effectively communicate results to stakeholders and leadership to improve the operational resilience of ICS environments.

Engineering, operations, and security professionals working in industrial environments and critical infrastructure sectors around the world are increasingly required to perform penetration tests and security assessments on key systems and devices. This course provides students with the necessary knowledge and skills to perform these tasks safely while ensuring operational reliability and resiliency and achieving effective cybersecurity outcomes.

ICS613 addresses the unique drivers and constraints of ICS environments and provides direct hands-on training to develop penetration testing and assessment capabilities specific to ICS devices, applications, architectures, communications, and process environments. By the end of this course, students will be equipped to perform real-world penetration tests and conduct security assessments of fully operational environments.

What You Will Receive

- A fully functional SANS ICS613 Student Kit that students will keep after class:
  - A CLICK PLC Plus Controller with Bluetooth and Wi-Fi, including additional modules and communication cards with a sector simulation board
  - Physical components and attachments for I/O connections to the SANS sector simulator board
  - Commercial Click PLC Programming software from KOYO Electronics
  - Commercial human machine interface (HMI) control system runtime applications from Rockwell Automation
  - Commercial OPC server application software from Matrikon
- A SANS ICS613 Windows Virtual Machine
- A SANS ICS613 Kali Virtual Machine
- Access to the in-class physical ICS range running a distributed control system (DCS) and automation components
- Unique custom tools that can be used for hardware and software asset data collection, industrial protocol network analysis, attack surface mapping, and ICS vulnerability validation

Section Descriptions

SECTION 1: Bench and Lab Testing

This section introduces the types of ICS/OT assessments, the risks and the three tenets of ICS/OT assessments. The section also introduces the three types of bench and lab testing for ICS/OT assessments, covering a high-level process of devices bench testing including hardware, firmware, administration and communication analysis.

TOPICS:

- Types of ICS/OT assessments
- Introduction to the bench testing assessment
- Bench and lab testing case studies, methodology and tool preparation
- Analyze device functionality, configuration and interfaces
- Hardware and firmware analysis including tools

SECTION 2: Preparing for ICS/OT Assessments

This section introduces passive and active security assessments for ICS/OT environments, covering how to define goals, choose an approach, apply threat intelligence and prepares students to plan, execute, and deliver safe and effective ICS/OT security assessments while emphasizing stakeholder collaboration.

TOPICS:

- Define assessment goals and outcomes and testing terminology
- Align with ICS/OT Cyber Kill Chain, Crown Jewel Analysis and threat intelligence
- Outline phased assessment methodology
- Collaborate with stakeholders
- Structure actionable test reports and balance mitigation options

SECTION 3: Top-Down Active Methodology

This section introduces a top-down penetration methodology aligned with the ICS/OT Cyber Kill Chain. Students learn to execute engagement objectives in simulated production environments using "living off the land" techniques while focusing on privilege escalation and OT boundary pivoting.

TOPICS:

- Follow assumed breach scenarios
- Master process enumeration
- Identify effective targets

SECTION 4: Security and Vulnerability Assessment

This section introduces passive security assessments for ICS/OT environments, covering nonintrusive techniques to collect and analyze the environment that align with industry standards. Students will learn ICS/OT specific knowledge and skills to analyze perimeters, network communications, hosts and active directory.

TOPICS:

- ICS/OT standard and frameworks alignment
- Common perimeter architectures and exploitable vectors
- ICS/OT vulnerability discovery and management
- Network analysis techniques
- Server and workstation analysis

SECTION 5: Bottom-Up Operations Assessment and Capstone

This section covers a bottom-up approach to ICS/OT attack identification aligned with the ICS/OT Cyber Kill Chain. Students learn to develop realistic attack scenarios with expected physical consequences, and demonstrate attacks in controlled environments, while emphasizing stakeholder collaboration.

The capstone allows students to apply all skills learned throughout the course in a comprehensive hands-on exercise against the ICS613 kit and in-class physical range, identifying vulnerabilities and recommending improvements to enhance ICS/OT defenses.

TOPICS:

- Various control system models and architectures
- Assess realistic attack scenarios and operational impacts
- Consequences and impacts to physical equipment
- Apply adversarial methods on targeting and TTPs
- Evaluate weaknesses and readiness of attack

Who Should Attend

- Cybersecurity professionals that have a mission to assess industrial environments
- Cybersecurity professionals that must conduct cyber assessments and pen tests for regulatory compliance
- ICS red/blue/hunt/incident responders/pentesters that are looking to enhance their individual and team capabilities
- Teams conducting assessments within Federal and DoD industrial facilities or weapon systems
- Cybersecurity professionals that are looking to gain experience in safely working with industrial devices and distributed control systems
- Experienced pentesters and cyber professionals that are looking to enhance their tradecraft and skills applied to the ICS domain

"Great course and a lot of great content discussion with tons of applicable, real-life thoughts, processes, examples, and in-depth descriptions."

—Jake K., **U.S. Government**